1. Buffer Overflow Attack Report!

Buffer overflows occur when a program attempts to write more data to a buffer than it can hold, potentially overwriting adjacent memory locations. This can be exploited by attackers to gain unauthorized access to systems or execute malicious code.

Report Guidelines:

Your task is to create a detailed blog post that covers various aspects of buffer overflow.

Methodology:

1. Define buffer overflows and their significance in computer security and briefly describe the potential consequences of buffer overflow attacks on systems and data.
2. Explain how buffer overflows occur, outlining the concept of overflowing data buffers and potential memory corruption.
3. Provide a simplified example of how an attacker might exploit a buffer overflow vulnerability.
4. Discuss the historical significance of buffer overflow attacks, citing real-world examples like the **Morris Worm** or **Heartbleed bug**.
5. Describe practical methods that can be used to reduce the risk of buffer overflow vulnerabilities in software

---

Submission Instructions:

1. Submit your report in a format suitable for sharing, create your report in Google Docs, ensuring it is well-organized and follows the guidelines provided.
2. Upon completion, adjust the sharing settings to **Anyone with the link can view**.
3. Submit the link to your report as part of your project completion.
4. Your posts should have examples and at least one picture, at the top. Publish your blog post on Medium and and share it at least LinkedIn.
5. Please, remember that these blogs must be written in English to further your technical ability in a variety of settings.

This task challenges you to delve into the world of buffer overflow attacks, understand their mechanisms and implications, and explore methods for safeguarding systems from such vulnerabilities.

https://medium.com/@SrN05/understanding-buffer-overflow-attacks-a-deep-dive-into-memory-corruption-2b59eb134c05